The Constantin-Rao Construction for Binary Asymmetric Error-Correcting Codes

R. J. McEliece
Consultant

E. R. Rodemich
Communications Systems Research Section

Recently Constantin and Rao gave an ingenious construction for a class of binary codes capable of correcting a single asymmetric error. In this article we shall give a complete analysis of the size of these codes.

I. Introduction

Most known classes of binary error-correcting codes have been designed for use on symmetric channels, i.e., channels for which the error probabilities 1 → 0 and 0 → 1 are equal. However, in certain applications (e.g., LSI memory protection (Ref. 1), optical communication (Ref. 6)), the observed errors are highly asymmetric, and the appropriate channel model may in fact be the Z-channel, in which the transition 0 → 1 is impossible. Of course any code capable of correcting t errors on a symmetric channel will also be capable of correcting t Z-channel errors; but at present there is no entirely satisfactory technique for dealing directly with asymmetric errors, comparable say to the BCH-Goppa construction (Ref. 5) for symmetric errors. Recently, however, Constantin and Rao (Ref. 1) gave an ingenious construction for a class of binary codes capable of correcting a single asymmetric error. Since our article is based on theirs, we begin with a description of the C.-R. codes.

Let V_n denote the set of binary n-tuples, and let G be any Abelian group of order $n + 1$. We suppose the nonzero elements of G are indexed $g^{(1)}, g^{(2)}, \cdots, g^{(n)}$. For each $\mathbf{x} = (x_1, \cdots, x_n) \in V_n$, we define

$$\gamma(\mathbf{x}) := \sum_{i=1}^{n} x_i g^{(i)} \tag{1}$$

the addition in Eq. (1) taking place in G. For each $g \in G$, define

$$V_n(g) := \{\mathbf{x} \in V_n : \gamma(\mathbf{x}) = g\} \tag{2}$$

Constantin and Rao showed that each of the subsets $V_n(g)$ is (qua code) capable of correcting one asymmetric error. They observed that since there are $n + 1$ sets $V_n(g)$, and since each of the 2^n elements of V_n belongs to exactly one of them, then

$$|V_n(g)| \geqslant \frac{2^n}{n+1}, \text{ for some } g \in G \tag{3}$$

Since $2^n/(n+1)$ is an *upper bound* on the cardinality of a single symmetric error-correcting code of length n, the simple bound of Eq. (3) already indicates that something interesting is afoot,[1] and one naturally wishes to know more about the numbers $|V'_n(g)|$. As a step in this direction, Constantin and Rao showed that

$$|V_n(0)| \geqslant |V_n(g)|, \text{ all } g \in G \tag{4}$$

in effect Eq. (4) eliminates the need to consider $V_n(g)$ for $g \neq 0$. However, this is as far as Constantin and Rao went; they were unable to find an exact formula for $|V_n(0)|$ except for certain special groups, and they did not identify the group or groups of order $n+1$ yielding the largest value of $|V_n(0)|$. We have been able to fill in these gaps using finite Fourier analysis. The details of our work appear in Sections II and III, but here we sketch our main conclusions.

First, we have obtained an explicit formula for $|V_n(g)|$ in general. The formula depends on the characters of G, and is given (with the change in notation noted below) in Theorem 1 of Section III. For $g = 0$, the case of primary interest, however, the formula simplifies to

$$|V'_n(0)| = \frac{1}{n+1} \sum_{h \text{ odd}} 2^{(n+1)/o(h) - 1} \tag{5}$$

the summation in Eq. (5) being extended over all elements $h \in G$ whose order $o(h)$ is odd. We can also show (Corollary 1, Section III) that the maximum of $|V_n(g)|$ is often not attained uniquely:

$$|V'_n(g)| \leqslant |V'_n(0)|, \text{ with equality if and only if } o(g) \text{ is a power of } 2.$$

In particular, if $n+1$ is a power of 2, all CR codes of length n have exactly $2^n/(n+1)$ codewords. Since this is also the number of words in the Hamming single (symmetric) error correcting code of the same length, we conclude that the CR construction is uninteresting for these lengths. However, it will follow from our results that for all other lengths, the CR construction produces codes that are strictly larger than the best single symmetric error correcting code.

We will also show (Corollary 2, Section III):

$$|V'_n(0)| \leqslant \frac{1}{n+1}\left(2^n + n2^{\frac{n-2}{3}}\right)$$

with equality if and only if $n+1$ is a power of 3 and G is an elementary Abelian 3-group. And finally, we will show (Corollary 3, Section III) that among all Abelian groups of order $n+1$, $|V'_n(0)|$ is maximized only by those groups whose odd Sylow subgroups are elementary Abelian.

Change in notation:

In what follows, the order of G will be denoted by n rather than $n+1$. Furthermore, in Section III we shall index the elements of G, *zero included*, as $G = \{g^{(0)}, g^{(1)}, \cdots, g^{(n-1)}\}$, and redefine the mapping $\gamma: V_n \to G$ by

$$\gamma(x) := \sum_{i=0}^{n-1} x_i g^{(i)}$$

We shall then study the numbers

$$f(g) := |\{x \in V_n : \gamma(x) = g\}|$$

The effect of this is that to translate our formulas for $f(g)$ into formulas for $|V'_n(g)|$, one must:

(1) Replace n by $(n+1)$.

(2) Divide the $f(g)$'s by 2.

Thus, for example, Corollary 1 in Section III reads $f(0) \leqslant 1/n \sum 2^{n/o(h)}$; using (1) and (2), we obtain $|V'_n(0)| \leqslant 1/(n+1) \sum 2^{(n+1)/o(h)-1}$, as claimed in Eq. (5).

II. Some Fourier Analysis

Let G be a finite Abelian group of order n, which we write additively. Then G is a direct sum of cyclic subgroups. This means that there exist elements $\gamma_1, \gamma_2, \cdots, \gamma_m$ in G of orders $n_1, n_2, \cdots, n_m$ with $n = n_1 n_2 \cdots n_m$, such that every element in G has a unique expansion of the form $g = g_1\gamma_1 + \cdots + g_m\gamma_m$, with $0 \leqslant g_i < n_i$, $i = 1, 2, \cdots, m$. For brevity, we write $g = (g_1, \cdots, g_m)$.

For each $i \in \{1, 2, \cdots, m\}$, let ζ_i be a complex primitive n_i-th root of unity. We define a mapping $\langle g, h\rangle$ of $G \times G$ into

[1] Indeed, if n is even, the maximum size for a single symmetric error-correcting code is $\leqslant 2^n/(n+2)$, and if $n \equiv 1 \pmod 4$, it is $\leqslant 2^n/(n+3)$. (See Ref. 4, Chapter 17.) Hence (3) shows that the best CR code of lengths $\equiv 0, 1, 2 \pmod 4$ has more codewords than any code designed to correct one symmetric error.

the complex numbers as follows. Let $g = (g_1, \cdots, g_m)$, $h = (h_1, \cdots, h_m)$.

$$\langle g, h\rangle : = \prod_{i=1}^{m} \zeta_i^{g_i h_i} \tag{6}$$

This mapping enjoys the following easily-checked properties.

$$\langle g, h\rangle = \langle h, g\rangle \tag{7}$$

$$\langle g, h\rangle \langle g, h'\rangle = \langle g, h + h'\rangle \tag{8}$$

$$\langle g, jh\rangle = \langle jg, h\rangle = \langle g, h\rangle^j \tag{9}$$

$$\sum_{g \in G} \langle g, h\rangle = \begin{matrix} 0 \text{ if } h \neq 0 \\ n \text{ if } h = 0 \end{matrix} \tag{10}$$

Now let $f(g)$ be any function mapping G into the complex numbers. The Fourier transform $\hat{f}$ of f is defined as follows:

$$\hat{f}(h) : = \sum_{g \in G} \langle h, -g\rangle f(g) \tag{11}$$

Using the properties of Eqs. (7), (8), and (10), it is easy to verify the Fourier inversion formula:

$$f(g) = \frac{1}{n} \sum_{h \in G} \langle h, g\rangle \hat{f}(h) \tag{12}$$

This is well-known and can be found, at least implicitly, in any good algebra text, e.g., Ref. 3, Chapter 1. We now derive an alternate version of Eq. (12), which is not as well-known, but which is often useful.

Let us call two elements h and h' of G *equivalent*, and write $h \sim h'$, if h and h' both generate the same cyclic subgroup of G. *From now on we shall assume that the Fourier transform $\hat{f}$ of f has the property that $\hat{f}(h) = \hat{f}(h')$ whenever $h \sim h'$.*

If $G = G_1 \cup G_2 \cup \cdots \cup G_r$ is the decomposition of G into "$\sim$" equivalence classes, and if $h_1, \cdots, h_r$ are arbitrary representatives of these classes, then Eq. (12) can be written as

$$f(g) = \frac{1}{n} \sum_{i=1}^{r} \hat{f}(h_i) \sum_{h \in G_i} \langle h, g\rangle \tag{13}$$

If h_i has order d_i, then every element $h \in G_i$ has the form $h = jh_i$ for some integer $1 \leqslant j \leqslant d_i$ with $(j, d_i) = 1$. Thus by Eq. (9) the inner sum in Eq. (13) is

$$\sum_{\substack{1 \leqslant j \leqslant d_i \\ (j, d_i) = 1}} \langle jh_i, g\rangle = \sum_{\substack{1 \leqslant j \leqslant d_i \\ (j, d_i) = 1}} \langle h_i, g\rangle^j \tag{14}$$

Now by Eq. (9), $\langle h_i, g\rangle$ is a complex e_i-th root of unity for a divisor e_i of d_i, and it follows from a theorem of Ramanujan (see Ref. 2, Theorem 272) that the sum (Eq. (14)) is equal to $\phi(d_i)\mu(e_i)/\phi(e_i)$, where ϕ is Euler's ϕ-function and μ is Mobius' function. Hence Eq. (13) becomes

$$f(g) = \frac{1}{n} \sum_{i=1}^{r} \phi(d_i) \frac{\mu(e_i)}{\phi(e_i)} \hat{f}(h_i) \tag{15}$$

Notice that if we define the product of $g = (g_1, \cdots, g_m)$ and $h = (h_1, \cdots, h_m)$ by

$$gh : = (g_1 h_1, \cdots, g_m h_m) \tag{16}$$

then the integer e_i appearing in Eq. (15) is just the order of the element gh_i. Thus if for $g \in G$ we define

$$|g| = \frac{\mu(e)}{\phi(e)}, \quad e = \text{order}(g) \tag{17}$$

Eq. (15) can be written as

$$f(g) = \frac{1}{n} \sum_{i=1}^{r} \phi(d_i) \, |gh_i| \, \hat{f}(h_i) \tag{18}$$

Finally we note that $|gh| = |gh_i|$ for all $h \in G_i$, and that $|G_i| = \phi(d_i)$, and so Eq. (18) can be written in either of the following ways:

$$f(g) = \frac{1}{n} \sum_{i=1}^{r} \phi(d_i) \, |h_j h_i| \, \hat{f}(h_i), \text{ if } g \sim h_j \tag{19}$$

$$f(g) = \frac{1}{n} \sum_{h \in G} |gh| \, \hat{f}(h) \tag{20}$$

III. Main Results

Let $G = \{g^{(0)}, g^{(1)}, \cdots, g^{(n-1)}\}$ be a finite Abelian group (we assume $g^{(0)} = 0$), and let V_n denote the set of n-tuples of 0's and 1's. For $\mathbf{x} = (x_0, x_1, \cdots, x_n) \in V_n$, define the mapping $\gamma: V_n \to G$ by

$$\gamma(\mathbf{x}) := \sum_{i=0}^{n-1} x_i g^{(i)} \tag{21}$$

Our problem is to count the number of times each element in G is covered in this mapping, i.e., to find the numbers

$$f(g) := |\{\mathbf{x} \in V_n : \gamma(\mathbf{x}) = g\}| \tag{22}$$

We will solve this problem by using the results of Section II. Here is the result:

Theorem 1:

For each $g \in G$,

$$f(g) = \frac{1}{n} \sum_{h \text{ odd}} \langle h, g \rangle\, 2^{n/o(h)} \tag{23}$$

In particular,

$$f(0) = \frac{1}{n} \sum_{h \text{ odd}} 2^{n/o(h)} \tag{24}$$

(In Eqs. (23) and (24), the symbol $o\,(h)$ denotes the order of the element $h \in G$, and the summation is extended over all elements in G of odd order.)

Proof:

This will follow from Eq. (12), once we compute $\hat{f}(h)$. From Eq. (11),

$$\hat{f}(h) = \sum_{g \in G} \langle h, -g \rangle f(g)$$

$$= \sum_{g \in G} \langle -h, g \rangle f(g) \qquad \text{(from Eq. (9))}$$

$$= \sum_{\mathbf{x} \in V_n} \langle -h, x_0 g^{(0)} + \cdots + x_{n-1} g^{(n-1)} \rangle \qquad \text{(from Eq. (22))}$$

$$= \prod_{i=0}^{n-1} (1 + \langle -h, g^{(i)} \rangle) \qquad \text{(from Eq. (8))}$$

One can easily see from Eq. (6) that for a fixed value of h, with $o(h) = d$, the mapping $g \to \langle -h, g \rangle$ is a homomorphism of G onto the complex d-th roots of unity. Thus if K denotes the product $\Pi_{i=0}^{d-1} (1 + \zeta^i)$, ζ being an appropriate primitive complex d-th root of unity, $\hat{f}(g) = K^{n/d}$. But the d complex numbers $\{1 + \zeta^i\}_{i=0}^{d-1}$ are roots of the equation $(z - 1)^d - 1 = 0$, and so their product is $1 - (-1)^d$, hence $K = 2$ if d is odd, $K = 0$ if d is even. Hence

$$\hat{f}(h) = 0 \quad \text{if } o(h) \text{ is even}$$

$$= 2^{n/o(h)} \quad \text{if } o(h) \text{ is odd} \tag{25}$$

and theorem 1 follows.

Corollary 1:

$$f(g) \leq f(0) = \frac{1}{n} \sum_{h \text{ odd}} 2^{n/o(h)}$$

with equality if and only if $o(g)$ is a power of 2.

Proof:

From Theorem 1,

$$f(g) = |f(g)| \leq \frac{1}{n} \sum_{h \text{ odd}} |\langle h, g \rangle|\, 2^{n/o(h)} \tag{26}$$

But $\langle h, g \rangle$, being a complex root of unity, has absolute value 1, and so

$$f(g) \leq \frac{1}{n} \sum_{h \text{ odd}} 2^{n/o(h)} = f(0) \tag{27}$$

This inequality will be equality, if and only if $\langle h, g \rangle = 1$ for all elements h of odd order. Now from Eq. (9) $\langle h, g \rangle$ will in general have an order which divides g.c.d. $(o(h), o(g))$. Hence if $o(g)$ is a power of 2, then $\langle h, g \rangle = 1$ for all h of odd order, and equality holds in Eqs. (26) and (27). Conversely if $o(g)$ is not a power of 2, then in the expansion $g = g_1 \gamma_1 + \cdots + g_m \gamma_m$, there will exist an index i such that $g_i \neq 0$, and $o(g_i \gamma_i)$ is not a power of 2. If $o(\gamma_i) = n_i = 2^a q$ with q odd, let $d = \text{g.c.d.}\,(2^a g_i, n_i)$. Then $d \not\equiv 0 \pmod{n_i}$ since $g_i \gamma_i$'s order is not a power of 2.

If the integer h_i is chosen so that $0 \leqslant h_i \leqslant n_i - 1$ and $(2^a g_i) h_i \equiv d \pmod{n_i}$, it follows that $h = 2^a h_i \gamma_i$ has odd order, and that

$$\langle h, g \rangle = \zeta_i^{2^a g_i h_i} = \zeta_i^d \neq 1. \qquad \text{QED.}$$

Corollary 2:

$f(0) \leqslant 1/n\,(2^n + (n-1)2^{n/3})$, with equality if and only if n is a power of 3, and G is an elementary Abelian 3-group.

Proof:

From Corollary 1,

$$f(0) = \frac{1}{n} \sum_{h \text{ odd}} 2^{n/o(h)}$$

$$= \frac{1}{n} \Bigl(2^n + \sum_{\substack{h \text{ odd} \\ h \neq 0}} 2^{n/o(h)}\Bigr)$$

If $h = 0$, but $o(h)$ is odd, then $o(h) \geqslant 3$. Hence $2^{n/o(h)} \leqslant 2^{n/3}$, and so

$$f(0) \leqslant \frac{1}{n} (2^n + (n-1)2^{n/3}) \tag{28}$$

Equality clearly holds in Eq. (29) if and only if every element in G (except 0) has order 3, i.e., iff G is an elementary Abelian 3-group. QED.

To state our final corollary, we need to introduce some number-theoretic notation. Let the prime-power decomposition of n be

$$n = \prod_{p \mid n} p^{e_p(n)} \tag{29}$$

and let P_1 be the set of odd primes dividing n. If π is a subset of P_1, we define

$$\alpha_\pi(n) := \prod_{p \in \pi} \left(p^{e_p(n)} - 1\right) \tag{30}$$

$$|\pi| := \prod_{p \in \pi} p \tag{31}$$

Corollary 3:

If G is a group of order n, then

$$f(0) \leqslant \frac{1}{n} \sum_{\pi \subseteq P_1(n)} \alpha_\pi(n) 2^{n/|\pi|} \tag{32}$$

with equality iff for all odd p, the Sylow p-subgroups of G are elementary Abelian.

Proof:

Let

$$G = \sum_{p \mid n} G_p$$

be the decomposition of G as the direct sum of its Sylow subgroups. If π is a subset of $P_1(n)$ let S_π be the subset of G consisting of these elements whose orders involve exactly the primes in π. Then clearly $|S_\pi| = \alpha_\pi(n)$, and every element in S_π has order at least $|\pi|$. The inequality of Eq. (32) follows. Furthermore, equality holds in Eq. (32) iff each element in each S_π has order exactly $|\pi|$, and this will happen iff each odd G_p is elementary. QED.

We conclude with one illustration of how Theorem 1 can be used to compute the values $f(g)$, for all $g \in G$. Suppose, then, that $G = Z_p \oplus Z_q$ is a direct sum of a cyclic p-group and a cyclic q-group, p and q being odd primes. We represent the elements of G as pairs (x, y), $0 \leqslant x < p$, $0 \leqslant y < q$. There are just four equivalence classes of elements in G, and we can choose as representatives of these classes (0, 0), (0, 1), (1, 0), (1, 1). The following table will prove useful:

i	h_i	d_i	$\phi(d_i)$	$\hat{f}(h_i)$
0	(0, 0)	1	1	2^{pq}
1	(0, 1)	q	$q - 1$	2^p
2	(1, 0)	p	$p - 1$	2^q
3	(1, 1)	pq	$(p-1)(q-1)$	2

Now what Eq. (19) says, in essence, is that the value $f(h_j)$ is the j-th component of the vector $\mathbf{f} = 1/n\, H\, \hat{\mathbf{f}}$, where H is the $r \times r$ matrix defined by

$$H_{ij} := \phi(d_i)\,[h_i h_j] \tag{33}$$

and $\hat{\mathbf{f}}$ is the column vector whose i-th component is $\hat{f}(h_i)$. In the present case, clearly

$$\mathbf{f}^T = (2^{pq}, 2^p, 2^q, 2)$$

and from the above table we compute

$$H = \begin{bmatrix} 1 & (q-1) & (p-1) & (p-1)(q-1) \\ 1 & -1 & (p-1) & -(p-1) \\ 1 & (q-1) & -1 & -(q-1) \\ 1 & -1 & -1 & +1 \end{bmatrix}$$

Hence

$$f(h_0) = \frac{1}{pq}\{2^{pq} + (q-1)2^p + (p-1)2^q + (p-1)(q-1)2\}$$

$$f(h_1) = \frac{1}{pq}\{2^{pq} - 2^p + (p-1)2^q - (p-1)2\}$$

$$f(h_2) = \frac{1}{pq}\{2^{pq} + (q-1)2^p - 2^q - (q-1)2\}$$

$$f(h_3) = \frac{1}{pq}\{2^{pq} - 2^p - 2^q + 2\}$$

For example with $p = 3$, $q = 5$, we get $f(h_0) = 2192$, $f(h_1) = 2188$, $f(h_2) = 2184$, $f(h_3) = 2182$. This means that the CR codes of length 14 defined by this group have

$$|V'_{14}(g)| = \begin{array}{l} 1096 \text{ if } g \sim h_0 \\ 1094 \text{ if } g \sim h_1 \\ 1092 \text{ if } g \sim h_2 \\ 1091 \text{ if } g \sim h_3 \end{array}$$

The best possible single symmetric error-correcting code of length 14 has only 1024 words (see Ref. 4, Appendix A).

References

1. Constantin, S. D. and T. R. N. Rao. "On the Theory of Binary Asymmetric Error-Correcting Codes," *Information and Control*, in press.
2. Hardy, G. M. and E. M. Wright, *An Introduction to the Theory of Numbers*, (4th ed.) London: Oxford University Press, 1960.
3. Lang, S. *Algebra*. Reading, Mass: Addison-Wesley, 1965.
4. MacWilliams, F. J. and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam: North-Holland Publishing Co., 1977.
5. McEliece, R. J. *The Theory of Information and Coding*. Reading, Mass: Addison-Wesley, 1976.
6. Pierce, J. R., "Optical Channels: Practical Limits with Photon Counting," *IEEE Trans. Communications COM-26* (1978), pp. 1819-1821.